The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/25/2019

SUBJECT:
Multiple Vulnerabilities in Mozilla Thunderbird Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Thunderbird versions prior to 68.2

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been identified in Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. Details of the vulnerabilities are as follows:

- A heap-based buffer over-read vulnerability in libexpat before 2.2.8 (CVE 2019-15903)
- A use-after-free vulnerability that results in a potentially exploitable crash (CVE 2019-11757)
- A memory safety bug when 360 Total Security is installed that could potentially be exploited to run arbitrary code (CVE 2019-11758)

- A stack-based buffer overflow that could potentially allow for arbitrary code execution (CVE 2019-11759)
- A stack-based buffer overflow in nrappkit that is potentially exploitable (CVE 2019-11760)
- A vulnerability that allows access to the privileged JSONView object (CVE 2019-11761)
- A vulnerability that allows for violation of document.domain origin isolation (CVE 2019-11762)
- A vulnerability in HTML entity parsing that could allow for XSS protection bypass (CVE 2019-11763)
- Memory safety bugs that could potentially be exploited to execute arbitrary code (CVE 2019-11764)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-35/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11764

https://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited